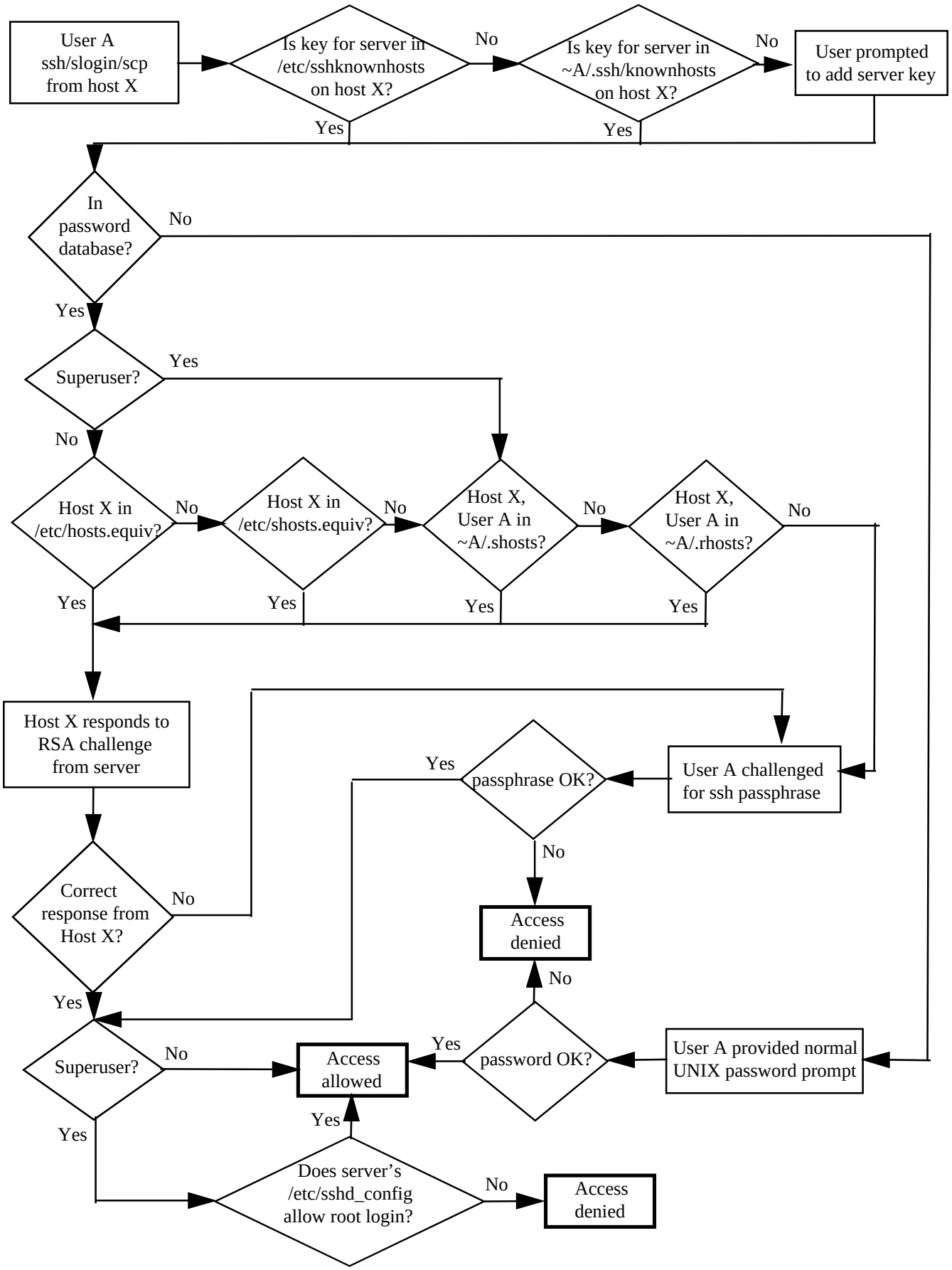
Flow for ssh/slogin/scp permissions in Freeware SSH 1.2.26 *(see notes)* TLS 03/11/99



NOTES

1 Like normal rlogin authentication, for any of the authorization files (/etc/hosts.equiv, /etc/shosts.equiv, ~/.rhosts and ~/.shosts) to permit access by a remote host, the name of that host must appear in the canonical form in the file; nicknames are not matched. For example, "seosparc1.gsfcmo.ecs.nasa.gov" would match, but "seosparc1" would not.

2 Entries for host keys in the ssh host authorization files (/etc/sshknownhosts and ~/.ssh/knownhosts) will only permit a session automatically if it is an exact match in both the local and remote knownhosts file.

Example for local (client) knownhosts file:
Keys are entered with the hostname in field 1 as the host was contacted the first time, but a match is looked for based on the current command line hostname. For example, if the first time you contacted host g0css02 you used "ssh g0css02", then the hostname in the key will be "g0css02". If you later try to do "ssh g0css02.gsfcb.ecs.nasa.gov" it will try to match the fully qualified name, fail, and then prompt you as to whether you want to add "g0css02.gsfcb.ecs.nasa.gov" to the list of known hosts. Note, however, that you can copy the entry for the host and edit field 1 to make it what you need.

Example for remote (server) knownhosts file:
You will be prompted for a passphrase if the entry in the server's knownhosts file does not exist or is not an exact match for the hostname used to verify the client.

3 Permissions on the authorization files (/etc/hosts.equiv, /etc/shosts.equiv, ~/.rhosts and ~/.shosts) are important. SSH will fail to permit remote logins if the permissions are 664, but will work if they are 644 or 600.

4 In our three environments (M&O, DAAC and SMC) home directories are automounted and shared *within* each environment for non-root users, and so one key for each environment is all that is needed. This is set up using the local scripts sshsetup and sshremote. In the case of root, however, each machine has its own /.ssh directory for root, and so a key for each machine must exist in the /.ssh/authorized_keys file. This will have to be done manually for now until we script something that will automate the task for when we cahnge passwords and passphrases. The steps would be:

- run sshsetup on each machine in an environment, providing same passphrase for root
- concatenate all of the /.ssh/identity.pub entries into one file
- distribute this concatenated file to each machine as /.ssh/authorized_keys

5 As of 11/98, the /etc/sshd_config file does not allow ssh, slogin or scp by root. The file is baselined with "PermitRootLogin no"and will require a CCR to make a change. If we want to be able to run root scripts using ssh we will have to make this change. Until then, files, permissions and root passphrases are not set up.